arXiv:math/0512244v1 [math.GR] 12 Dec 2005

F-QUASIGROUPS AND GENERALIZED MODULES

TOMÁŠ KEPKA*, MICHAEL K. KINYON, AND J. D. PHILLIPS

Abstract. In [3], we showed that every F-quasigroup is linear over a special kind of Moufang loop called an NK-loop. Here we extend this relationship by showing an equivalence between the equational class of (pointed) F-quasigroups and the equational class corresponding to a certain notion of generalized module (with noncommutative, nonassociative addition) for an associative ring.

1. Introduction

A *quasigroup* $(Q, \cdot)$ is a set Q with a binary operation $\cdot : Q \times Q \to Q$, denoted by juxtaposition, such that for each $a, b \in Q$, the equations $ax = b$ and $ya = b$ have unique solutions $x, y \in Q$. In a quasigroup $(Q, \cdot)$, there exist transformations $\alpha, \beta : Q \to Q$ such that $x\alpha(x) = x = \beta(x)x$ for all $x \in Q$. Now $(Q, \cdot)$ is called an *F-quasigroup* if it satisfies the equations

$$x \cdot yz = y \cdot \alpha(x)z \qquad \text{and} \qquad zy \cdot x = z\beta(x) \cdot yx$$

for all $x, y, z \in Q$.

If $(Q, \cdot)$ is a quasigroup, we set $M(Q) = \{a \in Q : xa \cdot yx = xy \cdot ax,\ \forall x, y \in Q\}$. If $(Q, \cdot)$ is an F-quasigroup, then $M(Q)$ is a normal subquasigroup of Q and $Q/M(Q)$ is a group [3, Lemma 7.5].

We denote by $\mathcal{F}_p$ the equational class (and category) of pointed F-quasigroups. That is, $\mathcal{F}_p$ consists of ordered pairs (Q, a), where Q is an F-quasigroup and $a \in Q$. We put $\mathcal{F}_m = \{(Q, a) \in \mathcal{F}_p : a \in M(Q)\}$.

A quasigroup with a neutral element is called a *loop*. Throughout this paper, we adopt an additive notation convention $(Q, +)$ (with neutral 0) for loops, although we do not assume that $+$ is commutative. The *nucleus* of a loop $(Q, +)$ is the set

$$N(Q, +) = \{a \in Q : \left\{ \begin{array}{c} (a + x) + y = a + (x + y) \\ (x + a) + y = x + (a + y) \\ (x + y) + a = x + (y + a) \end{array} \right\}, \forall x, y \in Q\}.$$

The *Moufang center* is the set

$$K(Q, +) = \{a \in Q : (a + a) + (x + y) = (a + x) + (a + y),\ \ \forall x, y \in Q\}.$$

Date: February 2, 2008.

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. F-quasigroup, Moufang loop, generalized modules.

*Partially supported by the institutional grant MSM 113200007 and by the Grant Agency of Charles University, grant #269/2001/B-MAT/MFF.

The intersection of the nucleus and Moufang center of a loop is the *center* $Z(Q,+) = N(Q,+) \cap K(Q,+)$. Each of the nucleus, the Moufang center, and the center is a subloop, and the center is, in fact, a normal subloop [1, 5].

A $(Q,+)$ will be called an *NK-loop* if for each $x \in Q$, there exist $u \in N(Q,+)$ and $v \in K(Q,+)$ such that $x = u + v$ $(= v + u)$. In other words, Q can be decomposed as a central product $Q = N(Q,+)\ K(Q,+)$. It was shown in [3] that every NK-loop is a Moufang A-loop. A *Moufang loop* is a loop satisfying the identity $((x+y)+x)+z = x+(y+(x+z))$ or any of its known equivalents [1, 5]. Every Moufang loop is *diassociative*, that is, the subloop generated by any given pair of elements is a group [4]. For a loop $(Q,+)$, the *inner mapping group* is the stabilizer of 0 in the group of permutations of Q generated by all left and right translations $L_x y = x + y = R_y x$. An *A-loop* is a loop such that every inner mapping is an automorphism [2].

In any Moufang A-loop $(Q,+)$, such as an NK-loop, the nucleus $N(Q,+)$ is normal (in fact, this is true in any Moufang loop), and $Q/N(Q,+)$ is a commutative Moufang loop of exponent 3. In particular, for each $x \in Q$, $3x \in N(Q,+)$, where $3x = x + x + x$. The Moufang center $K(Q,+)$ is also normal in Q (but this is not necessarily the case in arbitrary Moufang loops), and $Q/K(Q,+)$ is a group [3, Lemma 4.3]. In an NK-loop $(Q,+)$, we also have $Z(Q,+) = Z(N(Q,+)) = K(N(Q,+)) = Z(K(Q,+)) = N(K(Q,+))$. In addition, $K(Q,+) = \{a \in Q : a + x = x + a \ \ \forall x \in Q\}$.

The connection between F-quasigroups and NK-loops was established in [3].

Proposition. *For a quasigroup $(Q,\cdot)$, the following are equivalent:*

1. *$(Q,\cdot)$ is an F-quasigroup.*
2. *There exist an NK-loop $(Q,+)$, $f,g \in \mathcal{A}ut(Q,+)$, and $e \in N(Q,+)$ such that $x \cdot y = f(x) + e + g(y)$ for all $x,y \in Q$, $fg = gf$, and $x + f(x), x + g(x) \in N(Q,+)$, $-x + f(x), -x + g(x) \in K(Q,+)$ for all $x \in Q$.*

We refer to the data $(Q,+,f,g,e)$ of the proposition as being an *arithmetic form* of the F-quasigroup $(Q,\cdot)$. If (Q,a) is a pointed F-quasigroup in $\mathcal{F}_p$, then there is an arithmetic form such that $a = 0$ is the neutral element of $(Q,+)$.

The purpose of this paper is to extend the connection between (pointed) F-quasigroups and NK-loops further by showing an equivalence of equational classes between $\mathcal{F}_p$ and a certain notion of generalized module for an associative ring. Thus the study of (pointed) F-quasigroups effectively becomes a part of ring theory. The generalization we require weakens the additive abelian group structure of a module to an NK-loop structure.

Definition. *Let R be an associative ring, possibly without unity. A* generalized (left) R-module *is an NK-loop $(Q,+)$ supplied with an R-scalar multiplication $R \times Q \to Q$ such that the following conditions are satisfied: for all $a,b \in R$, $x,y \in Q$, $z \in N(Q,+)$, and $w \in K(Q,+)$,*

1. $\quad a(x+y) = ax + ay,$

2. $(a+b)x = ax + bx$,
3. $a(bx) = (ab)x$,
4. $ax \in K(Q,+)$,
5. $az \in N(Q,+)$, *and*
6. *there exists an integer* m *such that* $mw + aw \in Z(Q,+)$.

Here $mw = w + \cdots + w$ (m terms) is unambiguous by diassociativity.

If Q is a generalized R-module, then define the *annihilator* of Q to be $\mathrm{Ann}(Q) = \{a \in R : aQ = 0\}$. Clearly, $\mathrm{Ann}(Q)$ is an ideal of the ring R.

In order to state our main result, we need to describe a particular ring. Let $\mathbf{S} = \mathbb{Z}[\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}]$ be the polynomial ring in four commuting indeterminates $\mathbf{x}, \mathbf{y}, \mathbf{u}$, and $\mathbf{v}$ over the ring $\mathbb{Z}$ of integers. Put $\mathbf{R} = \mathbf{Sx} + \mathbf{Sy} + \mathbf{Su} + \mathbf{Sv}$, so that $\mathbf{R}$ is the ideal generated by the indeterminates. Clearly, $\mathbf{R}$ is a free commutative and associative ring (without unity) freely generated by the indeterminates.

Let $\mathcal{M}$ denote the equational class (and category) of generalized $\mathbf{R}$-modules Q such that:

1. $2z + \mathbf{x}z \in N(Q,+)$, $2z + \mathbf{y}z \in N(Q,+)$ for all $z \in Q$,
2. $\mathbf{x} + \mathbf{u} + \mathbf{xu} \in \mathrm{Ann}(Q)$, and
3. $\mathbf{y} + \mathbf{v} + \mathbf{yv} \in \mathrm{Ann}(Q)$.

Further, let $\mathcal{M}_p$ be the equational class (and category) of pointed objects from $\mathcal{M}$. That is, $\mathcal{M}_p$ consists of ordered pairs (Q,e), where $Q \in \mathcal{M}$ and $e \in Q$. Put $\mathcal{M}_n = \{(Q,e) \in \mathcal{F}_p : e \in N(Q,+)\}$, the equational class (and category) of *nuclearly* pointed objects from $\mathcal{M}$, and put $\mathcal{M}_c = \{(Q,e) \in \mathcal{F}_p : e \in Z(Q,+)\}$, the equational class (and category) of *centrally* pointed objects from $\mathcal{M}$.

Our main result is the following equivalence between pointed F-quasigroups and generalized $\mathbf{R}$-modules.

Main Theorem. *The equational classes* $\mathcal{F}_p$ *and* $\mathcal{M}_n$ *are equivalent. The equivalence restricts to an equivalence between* $\mathcal{F}_m$ *and* $\mathcal{M}_c$

2. Quasicentral endomorphisms

In this section, let $(Q,+)$ denote a (possibly non-commutative) diassociative loop. We endow the set $\mathcal{E}nd(Q,+)$ of all endomorphisms of $(Q,+)$ with the standard operations of addition, negation, and composition, *viz.*, for $f, g \in \mathcal{E}nd(Q,+)$, $f+g$ is defined by $(f+g)(x) = f(x) + g(x)$, $-f$ is defined by $(-f)(x) = -f(x) = f(-x)$, and fg is defined by $fg(x) = f(g(x))$ for all $x \in Q$.

An endomorphism f of $(Q,+)$ is called *central* if $f(Q) \subset Z(Q,+)$. We denote the set of all central endomorphisms of $(Q,+)$ by $\mathcal{Z}\mathcal{E}nd(Q,+)$. The verification of the following result is easy and omitted.

Lemma 2.1. *Let* $f, g, h \in \mathcal{Z}\mathcal{E}nd(Q,+)$ *be given. Then:*

1. $f + g \in \mathcal{Z}\mathcal{E}nd(Q,+)$,
2. $f + (g+h) = (f+g) + h$ *and* $f + g = g + f$,
3. *the zero endomorphism of* $(Q,+)$ *is central,*

4. $-f \in \mathcal{ZE}nd(Q,+)$,
5. $f + (-f) = 0$ *and* $f + 0 = f$.
6. $fg \in \mathcal{ZE}nd(Q,+)$,

Corollary 2.2. *$\mathcal{ZE}nd(Q,+)$ is an associative ring (possibly without unity) with respect to the standard operations.*

Let m be an integer. An endomorphism f of $(Q,+)$ is called *m-quasicentral* if $mx + f(x) \in Z(Q,+)$ for all $x \in Q$ (in which case $mx + f(x) = f(x) + mx$). An endomorphism is called *quasicentral* if it is m-quasicentral for at least one integer m. We denote by $\mathcal{QE}nd(Q,+)$ the set of all quasicentral endomorphisms of $(Q,+)$. The following is an obvious consequence of these definitions.

Lemma 2.3. 1. *An endomorphism is* 0*-quasicentral if and only if it is central,*
2. *$\mathcal{ZE}nd(Q,+) \subset \mathcal{QE}nd(Q,+)$, and*
3. *the identity automorphism,* Id_Q, *of $(Q,+)$ is (-1)-quasicentral.*

Lemma 2.4. *Let $f, g \in \mathcal{E}nd(Q,+)$.*

1. *If f is m-quasicentral and g is n-quasicentral, then fg is $(-mn)$-quasicentral.*
2. *If $f, g \in \mathcal{QE}nd(Q,+)$, then $fg \in \mathcal{QE}nd(Q,+)$.*

Proof. For (1): Fix $x \in Q$. Since f is m-quasicentral, $g(mx) + fg(x) = mg(x) + fg(x) \in Z(Q,+)$. Since g is n-quasicentral, $-mnx - mg(x) = -(g(mx) + nmx) \in Z(Q,+)$. Consequently,

$$\begin{aligned}-mnx + fg(x) &= ([-mnx - mg(x)] + mg(x)) + fg(x)\\ &= [-mnx - mg(x)] + [mg(x) + fg(x)] \in Z(Q,+).\end{aligned}$$

Thus, fg is $(-mn)$-quasicentral, as claimed.

(2) follows immediately from (1). □

Lemma 2.5. *Assume that $(Q,+)$ is commutative, let $f, g \in \mathcal{E}nd(Q,+)$ be m-quasicentral and n-quasicentral, respectively. Then*

1. *$-f$ is $(-m)$-quasicentral,*
2. *$f + g$ is an $(m+n)$-quasicentral endomorphism.*

In particular, for $f, g \in \mathcal{QE}nd(Q,+)$, $-f, f+g \in \mathcal{QE}nd(Q,+)$.

Proof. (1) is clear. For (2), set $z = (-mx - f(x)) + (-my - f(y)) + (-mx - g(x)) + (-my - g(y))$. Then $z \in Z(Q,+)$. It follows that

$$\begin{aligned}z + (f+g)(x+y) &= z + ([f(x) + f(y)] + [g(x) + g(y)]) = -mx - my - nx - ny\\ &= -mx - nx - my - ny = z + ([f(x) + g(x)] + [f(y) + g(y)])\\ &= z + ((f+g)(x) + (f+g)(y)).\end{aligned}$$

Thus $f+g \in \mathcal{E}nd(Q,+)$. Similarly, $(m+n)x + (f+g)(x) = [mx + f(x)] + [nx + g(x)] \in Z(Q,+)$. That is, (2) holds. □

Lemma 2.6. *Assume that $(Q,+)$ is commutative and let $f, g, h \in \mathcal{QE}nd(Q,+)$. Then*

1. $f + g = g + f$,
2. $f + (g + h) = (f + g) + h$,
3. $f + (-f) = 0$, *and*
4. $f + 0 = f$.

Proof. (1), (3), and (4) are obvious. For (2): There exist $m, n, k \in \mathbb{Z}$ such that $mx + f(x), nx + g(x), kx + h(x) \in Z(Q, +)$. Set $y = (-f(x) - mx) + (-g(x) - nx) + (-h(x) - kx)$. Then $y \in Z(Q, +)$ and $y + (f(x) + (g(x) + h(x))) = -(m+n+k)x = y + ((f(x) + g(x)) + h(x))$ for all $x \in Q$. □

Corollary 2.7. *If $(Q, +)$ is commutative, then $\mathcal{QE}nd(Q, +)$ is an associative ring with unity.*

We conclude this section with a straightforward observation.

Lemma 2.8. *Assume that for $k \in \{1, 2, 3\}$, $kx \in Z(Q, +)$ for all $x \in Q$. Then*
1. *Every quasicentral endomorphism is m-central for some $m \in \{0, 1, -1\}$,*
2. *If $f \in \mathcal{QE}nd(Q, +) \cap \mathcal{A}ut(Q, +)$, then $f^{-1} \in \mathcal{QE}nd(Q, +)$.*

3. Special endomorphisms of NK-loops

In this section, let $(Q, +)$ be an NK-loop. We denote by N, K, and Z the underlying sets of $N(Q, +)$, $K(Q, +)$, and $Z(Q, +)$, respectively. As noted in §1, $Z(Q, +) = Z(N, +) = Z(K, +)$ and $Z = N \cap K$.

An endomorphism f of $(Q, +)$ will be called *special* if $f(Q) \subset K$, $f|_K$ is a quasicentral endomorphism of $(K, +)$, and $f(N) \subset N$. Then $f|_N$ is a central endomorphism of $(N, +)$ and $f(N) \subset Z$. We denote by $\mathcal{SE}nd(Q, +)$ the set of special endomorphisms of $(Q, +)$.

Lemma 3.1. *Let $f, g, h \in \mathcal{SE}nd(Q, +)$. Then*
1. $fg \in \mathcal{SE}nd(Q, +)$,
2. $f + g \in \mathcal{SE}nd(Q, +)$, *and* $f + g = g + f$,
3. $f + (g + h) = (f + g) + h$,
4. $-f \in \mathcal{SE}nd(Q, +)$, $f + (-f) = 0$, *and* $f + 0 = f$.

Proof. For (1), use Lemma 2.4.

For (2): Take $x, y \in Q$. Then $x = a + b$ and $y = c + d$ for some $a, c \in N, b, d \in K$ so that

$$\begin{aligned} u = (f + g)(x + y) &= f(x + y) + g(x + y) = [f(x) + f(y)] + [g(x) + g(y)] \\ &= [(f(a) + f(b)) + (f(c) + f(d))] + [(g(a) + g(b)) + (g(c) + g(d))] \end{aligned}$$

and

$$\begin{aligned} v = (f + g)(x) + (f + g)(y) &= [f(x) + g(x)] + [f(y) + g(y)] \\ &= [(f(a) + f(b)) + (g(a) + g(b))] + [(f(c) + f(d)) + (g(c) + g(d))]. \end{aligned}$$

The restrictions $f|_N$ and $g|_N$ are central endomorphisms of $(N, +)$, and it follows that $f(N) \cup g(N) \subset Z(N, +) = Z(Q, +)$. Thus, $f(a), f(c), g(a), g(c) \in Z$ and in

order to check that $u = v$ it is sufficient to show that $(f(b) + f(d)) + (g(b) + g(d)) = (f(b)+g(b))+(f(d)+g(d))$. However, the latter equality holds, since the restrictions $f|_K$ and $g|_K$ are quasicentral endomorphisms of the commutative loop $(K, +)$ and Corollary 2.7 applies.

We have shown that $f + g \in \mathcal{E}nd(Q, +)$. The facts that $f + g$ is special and $f + g = g + f$ are easily seen, using Lemma 2.6 applied to the loop $(K, +)$.

For (3): Using the facts that $(Q, +)$ is an NK-loop and $f(N) \cup g(N) \cup h(N) \subset Z$, it is enough to show that $f(u) + (g(u) + h(u)) = (f(u) + g(u)) + h(u)$ for all $u \in K$. Now we proceed similarly as in the proof of Lemma 2.6.

Finally, (4) is easy. □

Corollary 3.2. *$\mathcal{SE}nd(Q, +)$ is an associative ring (possibly without unity).*

An endomorphism f of $(Q, +)$ will be said to satisfy *condition (F)* if

$$-x + f(x) \in K \qquad \text{and} \qquad x + f(x) \in N$$

for all $x \in Q$. Then $f(K) \subset K$ and $f(N) \subset N$.

Lemma 3.3. *Let $f \in \mathcal{E}nd(Q, +)$ satisfy* (F). *Define $h : Q \to Q$ by $h(x) = -x+f(x)$ for all $x \in Q$. Then $h \in \mathcal{SE}nd(Q, +)$.*

Proof. First we check that $h \in \mathcal{E}nd(Q, +)$. Fix $x, y \in Q$ with $x = a + b$, $y = c + d$, $a, c \in N$, $b, d \in K$. Set $u = h(x + y)$, $v = h(x) + h(y)$, and $w = (a - f(a)) + (c - f(c)) + (-b - f(b)) + (-d - f(d))$. Then $w \in Z$,

$$u = (-y - x) + f(x + y) = ((-d - c) + (-b - a)) + ((f(a) + f(b))) + (f(c) + f(d))$$

and

$$v = (-x+f(x))+(-y+f(y)) = (-b-a)+(f(a)+f(b))+((-d-c)+(f(c)+f(d))).$$

On the other hand,

$$\begin{aligned}
u + w &= [(-d - c) + (-b - a)] + [(a - b) + (c - d)] \\
&= [(-d - c) - b] + [-a + (a - b)] + (c - d) \\
&= [(-d - c) - b] + [(c - d) - b] \\
&= [(-d - c) + (c - d)] - 2b \\
&= -2d - 2b \\
&= -2(b + d) \\
&= [(-b - a) + (a - b)] + [(-d - c) + (c - d)] \\
&= v + w.
\end{aligned}$$

Consequently, $u = v$, so that $h \in \mathcal{E}nd(Q, +)$, as claimed. Further, it follows immediately from the definition of h that $h(Q) \subset K$ and $h(N) \subset N$ (then $h(N) \subset Z$). Finally, $2a + h(a) = a + f(a) \in Z$ for all $a \in K$, and therefore $h|_K$ is a 2-quasicentral endomorphism of $(K, +)$. Thus $h \in \mathcal{SE}nd(Q, +)$. □

Lemma 3.4. *Let $f, g \in \mathcal{E}nd(Q,+)$ satisfy* (F)*. Define $h, k : Q \to Q$ by $h(x) = -x + f(x)$ and $k(x) = -x + g(x)$ for all $x \in Q$. Then $hk = kh$ if and only if $fg = gf$.*

Proof. By Lemma 3.3, $h \in \mathcal{E}nd(Q,+)$, and hence

$$hk(x) = h(-x + g(x)) = -h(x) + hg(x) = (-f(x) + x) + (-g(x) + fg(x)).$$

On the other hand,

$$kh(x) = -h(x) + gh(x) = (-f(x) + x) + (-g(x) + gf(x))$$

by the definition of h and k. The result is now clear. □

Lemma 3.5. *Let $f, g \in \mathcal{A}ut(Q,+)$ satisfy* (F)*. Define $h, k, p, q : Q \to Q$ by $h(x) = -x + f(x)$, $k(x) = -x + g(x)$, $p(x) = -x + f^{-1}(x)$, and $q(x) = -x + g^{-1}(x)$ for all $x \in Q$. Then*

1. *$h, k, p, q \in \mathcal{SE}nd(Q,+)$,*
2. *$hp = ph$ and $h + p + hp = 0$,*
3. *$kq = qk$ and $k + q + kq = 0$, and*
4. *If $fg = gf$, then the endomorphisms h, k, p, q commute pairwise.*

Proof. (1) follows from Lemma 3.3.

For (2): We have $ff^{-1} = f^{-1}f$ and hence $hp = ph$ by Lemma 3.4. Now, put $A = h + p + hp$. Then A is a (special) endomorphism of $(Q,+)$ and $A(x) = [-x + f(x)] + [-x + f^{-1}(x)] + [(-f^{-1}(x) + x) + (-f(x) + x)]$. Clearly, $N \subset \ker(A)(= \{u \in Q : A(u) = 0\})$. On the other hand, if $x \in K$, then $-x + f(x), -x + f^{-1}(x) \in Z$ and the equality $A(x) = 0$ is clear, too. Thus, $N \cup K \subset \ker(A)$. But $(Q,+)$ is an NK-loop and $\ker(A)$ is a subloop of $(Q,+)$. It follows $\ker(A) = Q$ and $A = 0$.

(3) is proven similarly to (2).

For (4), combine (2), (3), and Lemma 3.4. □

4. The equivalence

We now turn to the proof of the Main Theorem. First, recall the definition of generalized module over a ring R, and observe that the conditions (1), (4), (5), and (6) of the definition imply that for each $a \in R$, the transformation $Q \to Q; x \mapsto ax$ is a special endomorphism of $(Q,+)$. Recall also the ring $\mathbf{R}$, which is the ideal of $\mathbf{S} = \mathbb{Z}[\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}]$ freely generated by the commuting indeterminates $\mathbf{x}, \mathbf{y}, \mathbf{u}$, and $\mathbf{v}$.

First, take $(Q, a) \in \mathcal{F}_p$. As described in §1, let $(Q, +, f, g, e)$ be the arithmetic form of the F-quasigroup $(Q, \cdot)$ such that $a = 0$ in $(Q,+)$. Then $f, g \in \mathcal{A}ut(Q,+)$ satisfy condition *(F)*. Further, define $\varphi, \mu, \psi, \nu : Q \to Q$ by $\varphi(x) = -x + f(x)$, $\mu(x) = -x + f^{-1}(x)$, $\psi(x) = -x + g(x)$, and $\nu(x) = -x + g^{-1}(x)$ for all $x \in Q$. By Lemma 3.5, the special endomorphisms φ, ψ, μ, and ν of the loop $(Q,+)$ commute pairwise, and $\varphi + \mu + \varphi\mu = 0 = \psi + \nu + \psi\nu$. Consequently, these endomorphisms generate a commutative subring of the ring $\mathcal{SE}nd(Q,+)$ (see Corollary 3.2) and there exists a (uniquely determined) homomorphism $\lambda : \mathbf{R} \to \mathcal{SE}nd(Q,+)$ such that $\lambda(\mathbf{x}) = \varphi$, $\lambda(\mathbf{y}) = \psi$, $\lambda(\mathbf{u}) = \mu$, and $\lambda(\mathbf{v}) = \nu$. The homomorphism λ induces

an $\mathbf{R}$-scalar multiplication on the loop $(Q,+)$, and the resulting generalized $\mathbf{R}$-module will be denoted by $\overline{Q}$. By Lemma 3.5, $\lambda(\mathbf{x}+\mathbf{u}+\mathbf{xu}) = 0 = \lambda(\mathbf{y}+\mathbf{v}+\mathbf{yv})$, and so $\mathbf{x}+\mathbf{u}+\mathbf{xu}, \mathbf{y}+\mathbf{v}+\mathbf{yv} \in \mathrm{Ann}(Q)$. Also, since f, g satisfy *(F)*, we have $2z+\lambda(\mathbf{x})z = 2z+\varphi(z) = z+f(z) \in N(Q,+)$ and similarly $2z+\lambda(\mathbf{y})z \in N(Q,+)$ for all $z \in Q$. It follows that $\overline{Q} \in \mathcal{M}$. Now define $\rho : \mathcal{F}_p \to \mathcal{M}_n$ by $\rho(Q,a) = (\overline{Q}, e)$, and observe that $(\overline{Q}, e) \in \mathcal{M}_c$ if and only if $e \in Z(Q,+)$.

Next, take $(\overline{Q}, e) \in \mathcal{M}_n$ and define $f, g : Q \to Q$ by $f(z) = z + \mathbf{x}z$ and $g(z) = z + \mathbf{y}z$ for all $z \in Q$. We have $f(x+y) = (x+y) + (\mathbf{x}x + \mathbf{x}y)$ and $f(x)+f(y) = (x+\mathbf{x}x)+(y+\mathbf{x}y)$. Further, $x = u_1+v_1$, $y = u_2+v_2$ for some $u_1, u_2 \in N(Q,+)$, $v_1, v_2 \in K(Q,+)$, and hence, $f(x+y) = (u_1+u_2+v_1+v_2)+(\mathbf{x}u_1+\mathbf{x}u_2+\mathbf{x}v_1+\mathbf{x}v_2)$, and $f(x)+f(y) = (u_1+\mathbf{x}u_1+v_1+\mathbf{x}v_1)+(u_2+\mathbf{x}u_2+v_1+\mathbf{x}v_2)$. But $\mathbf{x}u_1, \mathbf{x}u_2 \in Z(Q,+)$, and so in order to show $f(x+y) = f(x)+f(y)$, it is enough to check that $(v_1+v_2)+(\mathbf{x}v_1+\mathbf{x}v_2) = (v_1+\mathbf{x}v_1)+(v_2+\mathbf{x}v_2)$. However, $-2v_1 - \mathbf{x}v_1 \in Z(Q,+)$ and $-2v_2 - \mathbf{x}v_2 \in Z(Q,+)$, and so the latter equality is clear.

We have proven that $f \in \mathcal{E}nd(Q,+)$, and the proof that $g \in \mathcal{E}nd(Q,+)$ is similar. Now by definition of generalized module, $-x+f(x) = \mathbf{x}x \in K(Q,+)$ and $-x+g(x) = \mathbf{y}x \in K(Q,+)$ for all $x \in Q$. By definition of $\mathcal{M}$, $x+f(x) = 2x+\mathbf{x}x \in N(Q,+)$ and $x+g(x) = 2x+\mathbf{y}x \in N(Q,+)$ for all $x \in Q$. This means that both f and g satisfy *(F)* and it follows from Lemma 3.4 that $fg = gf$.

Define $h : Q \to Q$ by $h(x) = x + \mathbf{u}x$ for $x \in Q$. We have $\mathbf{u}x + \mathbf{x}x + \mathbf{xu}x = 0$, and so $\mathbf{x}x + \mathbf{xu}x = -\mathbf{u}x$. Now, $fh(x) = h(x) + \mathbf{x}h(x) = (x+\mathbf{u}x)+(\mathbf{x}x+\mathbf{xu}x) = (x+\mathbf{u}x) - \mathbf{u}x = x$ and $fh = \mathrm{Id}_Q$. Similarly, $hf = \mathrm{Id}_Q$ and we see that $f \in \mathcal{A}ut(Q,+)$. Similarly, $g \in \mathcal{A}ut(Q,+)$.

We have that $f, g \in \mathcal{A}ut(Q,+)$, and $e \in Q$ satisfy the conditions of the Proposition of §1, and so defining a multiplication on Q by $xy = f(x)+e+g(y)$ for all $x, y \in Q$ gives an F-quasigroup. Define $\sigma : \mathcal{M}_n \to \mathcal{F}_p$ by $\sigma(\overline{Q}, e) = (Q, 0)$.

It is easy to check that the operators ρ and σ represent an equivalence between $\mathcal{F}_p$ and $\mathcal{M}_n$. Further, $0 \in \mathcal{M}(Q)$ if and only if $e \in Z(Q,+)$, so that ρ and σ restrict to an equivalence between $\mathcal{F}_m$ and $\mathcal{M}_c$. This completes the proof of the Main Theorem.

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer-Verlag, 1971.
[2] R. H. Bruck and L. Paige, Loops in which every inner mapping is an automorphism, *Ann. of Math.* **63** (1956), 308–323.
[3] T. Kepka, M. K. Kinyon, and J. D. Phillips, The structure of F-quasigroups, submitted, `math.GR/0510298`.
[4] R. Moufang, Zur struktur von alternativkorpern, *Math. Ann.* **110** (1935), 416–430.
[5] H. O. Pflugfelder, *Quasigroups and Loops, Introduction*, Helderman-Verlag, 1990.

Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic
E-mail address: kepka@karlin.mff.cuni.cz

Department of Mathematical Sciences, Indiana University South Bend, South Bend, IN 46634 USA
E-mail address: mkinyon@iusb.edu
URL: http://mypage.iusb.edu/~mkinyon

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933 USA
E-mail address: phillipj@wabash.edu
URL: http://www.wabash.edu/depart/math/faculty.html#Phillips